問3　転職サイトにおける個人情報保護に関する次の記述を読んで，設問1，2に答えよ。

P社は，従業員数30名の人材紹介会社である。コンサルタントによる人材紹介だけでなく，転職サイトも立ち上げている。この転職サイトには，求職者，求人企業が多数，登録している。求職者は，転職サイトの個人プロフィール登録画面で，氏名，生年月日，住所，電話番号，職歴などの個人プロフィールを登録する。求職者の転職サイトの利用は無料である。求人企業は，業種，募集職種，職務内容，給与，勤務地，応募資格などの求人募集内容の掲載をP社に依頼する。求人企業は，求人募集時には求人件数に応じた利用料を，採用成立時には紹介料をP社に支払う。

〔求職者の個人情報の保護〕

求職者は，求人募集内容を見て応募したい求人企業があれば，転職サイト内のそれぞれの求人企業の応募入力画面を利用して応募することができる。応募入力画面では，あらかじめ個人プロフィール登録画面で登録しておいた個人プロフィールをそのまま利用することもできるが，新たに入力することもできる。さらに，各求人企業に対する応募理由などを追加入力することもできる。この応募時の個人プロフィールは，P社のWebサーバから，求人企業に，電子メール（以下，メールという）で自動送信される。

なお，求職者の個人情報を求人企業に提供することについては，求職者から事前に転職サイトの画面で同意を得ており，また，求人企業に対しても提供する個人情報の利用目的を利用規約で制限しており，特に問題ないとP社は認識している。

求人企業のうち，数社から，暗号化されていないメールで求職者の個人情報を送信することについて，漏えいする危険性があるので改善してほしいとの要望があった。これを受けて，P社の情報システム部のF部長は，システム担当のZ主任に，メールが盗聴される危険性を踏まえた改善案を作成するよう命じた。

Z主任は，F部長の指示に従って，改善案を表1にまとめた。

表１　個人情報を含むメールが盗聴される危険性を踏まえた改善案

	案１	案２	案３
方式	メールの暗号化	パスワード付きファイルの添付	求人企業向け Web ページの追加
実現手段	個人プロフィールを送信するメールを S/MIME 又は PGP を用いて暗号化する。	個人プロフィールを含む文書ファイルなどをパスワードで保護した状態でメールに添付して送信する。	応募があったときに，個人プロフィールを含めず，応募があったことだけを通知するメールを送信する。求人企業は，パスワード認証と TLS（SSL）で保護されている求人企業向け Web ページから個人プロフィールをダウンロードする。
利点	秘匿性が高い。	ほとんどの求人企業で利用可能である。	メールに個人情報を含まない。
欠点	S/MIME，PGP は，求人企業に普及していない。	秘匿性が低い。パスワードの管理が必要となる。	求人企業の利用者が個人プロフィールにアクセスする際の手順が増える。パスワードの管理が必要となる。

次は，各案を比較した際の F 部長と Z 主任の会話である。

Z 主任 ：案１の S/MIME はどうでしょうか。

F 部長 ：S/MIME は，各求人企業が［　a　］を用意するために認証サービスを年間契約することなどが必要である。コストが掛かるから難しいだろう。

Z 主任 ：各求人企業が自社で［　a　］を発行する方法は，採用できないのでしょうか。

F 部長 ：①各求人企業が自社で発行したものは，当社では［　a　］として受け入れられない。

Z 主任 ：当社で認証局システムを構築して，求人企業の各利用者分も含めて［　a　］を発行するのはどうでしょうか。

F 部長 ：その場合，導入コストに加えて運用コストも必要だ。

Z 主任 ：それでは，PGP はどうでしょうか。

F 部長 ：PGP は，自社で鍵の生成システムを用意できるとしても，クライアント PC の［　b　］ソフトが対応していないことが多く，操作手順が複雑になるので，一般の利用者には使いにくいだろう。案１の採用は難しいようだね。

Z 主任 ：案２はどうですか。

F 部長 ：もし攻撃者が添付ファイルを入手したら，総当たり攻撃をかけることができるので，パスワードは十分に長くしないといけないね。

Z主任：最短パスワード長は，8文字でどうでしょうか。

F部長：それでは足りないだろう。サーバへのログインのように，②オンラインでパスワードを入力させる場合は，試行回数を多くできないように制限することもできるから8文字程度でも十分な場合が多い。しかし，案2の場合は，添付ファイルを攻撃者に入手されたら，ファイルに対してオフラインで直接的に攻撃されて試行回数が制限できない上に，解析ツールを利用して，ごく短時間でパスワードを解析される危険性もある。だから，パスワードはかなり長くする必要があるが，運用上はなかなか難しいだろう。

Z主任：そうすると，案3でしょうか。

F部長：そうだね。案3は，求人企業の利用者の手間が増えるという欠点はあるが，この欠点は操作性の高い求人企業向けWebページを用意することによって補うことができるだろう。また，当社で求人企業の利用者の初期パスワードを管理する必要があるが，求人企業の利用者の総数から考えて，大きな手間にはならないだろう。

F部長とZ主任は，案3を採用することにした。求人企業向けWebページの操作性については，求職者の個人プロフィールを簡単な手順で確認できるように設計することにした。

P社では，求人企業向けWebページを追加し，各求人企業に運用方法の変更を通知した上で，案3に沿った運用方法に切り替えた。

〔求人企業向けWebページのパスワード〕

求人企業向けWebページでは，表2に示すような利用者IDとパスワードを求人企業の利用者ごとに発行し，各求人企業向けのWebページだけにアクセスできるようになっている。求人企業の利用責任者は，最初にP社に依頼するときに，各利用者のメールアドレスを含む申込書と，求人企業の登記事項証明書を郵送する。P社では，利用者IDは求人企業の各利用者にメールで送信するが，③初期パスワードの通知書は登記事項証明書に記載された所在地気付で利用責任者あてに一括して郵送している。求人企業の各利用者は，初めて求人企業向けWebページにログインしたときには，パスワードを変更してから利用する。

なお，初期パスワードの通知書は，パスワードを変更した後も，各利用者が保管するようにP社からお願いしている。

表2　求人企業向けWebページの利用者IDとパスワード

項目	生成方法／設定方法	例
利用者ID	P社が，求人企業の利用者に対して，登録順に1人に一つずつ割り振る連続番号（数字8けた）。	00000099
初期パスワード	利用者IDを3倍した数字の下8けたと，発行日（西暦4けた，月2けた，日2けた）を合わせた16けたの数字。	0000029720100405
パスワード	初回ログイン時に，求人企業の利用者が設定する。8けた以上の文字列で，英字，数字，記号が使用可能。	A9d3&jw27

このような方法で運用していたところ，求人企業のQ社から3名の利用者を含む申込みがあり，各利用者の初期パスワードを利用責任者あてに郵送した。その3名の初期パスワードを見たQ社の利用責任者は，④他人の初期パスワードを推定可能であるという問題があると，P社に指摘した。F部長とZ主任は，その指摘に対して，直ちに改善を行った。

また，別の問題点として，パスワード変更後にパスワードを忘れたという問合せがしばしば発生するようになった。そこで，Z主任は，図のようなパスワード再設定手順を追加することを考え，F部長に提案した。

(1)　求人企業の利用者が，パスワード再設定の申請ページに利用者IDを入力する。
(2)　Webアプリケーションが自動的に，パスワード再設定の申請があった旨と，パスワード再設定の実行ページのURLを，P社に登録されている利用者のメールアドレスあてにメールで通知する。第三者からのアクセスを避けるためにURLには十分に長いランダムな文字列を含める。
(3)　求人企業の利用者が，URLの示すパスワード再設定の実行ページにアクセスし，新パスワードを入力すると新パスワードが設定される。
(4)　パスワード再設定の実行ページのURLを通知後，20分以内にアクセスがない場合は，実行ページのURLを自動的に無効にする。

図　求人企業向けWebページのパスワード再設定手順（当初案）

F部長は，⑤図のパスワード再設定手順では第三者にパスワードを再設定されてしまう危険性があることを指摘し，Z主任に対応を指示した。Z主任は，F部長の指示に従い，⑥パスワード再設定手順を見直し，再提案した。

その後，P社では，Z主任の再提案を採用して，見直し後のパスワード再設定手順での運用を開始した。

設問1　〔求職者の個人情報の保護〕について，(1)～(4)に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を，［ a ］については10字以内で，［ b ］については5字以内で答えよ。

(2) F部長が，本文中の下線①のように述べている理由を30字以内で述べよ。

(3) PGPでは，通常，証明書のフィンガプリントを確認するが，正しいフィンガプリントの入手方法として安全と考えられるものを一つ挙げ，30字以内で述べよ。

(4) 本文中の下線②を実現する対策の内容を50字以内で具体的に述べよ。

設問2　〔求人企業向けWebページのパスワード〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，初期パスワードの通知書の郵送先を求人企業の登記事項証明書に記載された所在地としたP社の意図は何か。40字以内で述べよ。

(2) 本文中の下線④について，問題を解決するためには初期パスワードをどのように生成すればよいか。30字以内で述べよ。

(3) 本文中の下線⑤について，総当たり攻撃以外には，どのような手口で第三者にパスワードを再設定されてしまうか。40字以内で述べよ。

(4) 本文中の下線⑥について，Z主任の考えた見直し案はどのようなものであったと考えられるか。40字以内で述べよ。